North Carolina HIE Privacy and Security Policies
January 18, 2011

1. Scope of Rules

   (a) Defining “exchange through the HIE”
   (b) Application to regional exchanges connecting to HIE

Privacy

2. Patient Opt Out Rights

   (a) Content of opt out and revocation forms
   (b) Patient notice and education
   (c) Process for collecting forms
   (d) Process for implementing requests
   (e) Record retention
   (f) Scope of opt out (i.e., definition of individual provider)

3. Purposes for Access by Covered Entities

   (a) Defining treatment, payment and health care operations
   (b) Procedures for verifying appropriate patient relationships

4. Compliance With Minimum Necessary Requirement

   (a) Scope of minimum necessary requirement
   (b) Reliance by disclosing entities on requests by accessing entities
   (c) Obligations of accessing entities

5. Break the Glass

   (a) Types of entities granted break the glass rights
   (b) Break the glass certification language
   (c) Process for tracking break the glass incidents

6. Access to Data by HIE Staff

   (a) Permissible purposes (auditing, system maintenance, breach investigation, etc.)
   (b) Levels of access for HIE staff

7. Access to Data by Researchers

   (a) Creation of HIE IRB or privacy board
   (b) Standards for granting access to researchers

8. Access to Data by Government Agencies

   (a) Public health authorities
   (b) Other (health system oversight, law enforcement, etc.)

9. Access to De-identified Data

   (a) Definition of "de-identified"
   (b) Safeguards for preventing re-identification
   (c) Process for granting requests for access

10. Responding to Subpoenas and Discovery Requests

11. Implementation of Restrictions on Payer Access

12. Tracking of Disclosures by HIE for Accounting Purposes

13. Patient Access to Data

   (a) Will HIE create patient portal or other access rights?
   (b) Process for handling patient access requests
   (c) Access to minors' data by parents and guardians

Security

14. Authorization Controls

   (a) Process for granting covered entities access rights
   (b) Process and standards for granting business associates access rights
   (c) User categories within covered entities and business associates
   (d) User rights by category
   (e) Process for terminating rights of covered entities, business associates and users

15. Authentication

   (a) Gateway (entity-level) authentication procedures (e.g. procedures for administering digital credentials and requirement for use)
   (b) Individual (user-level) authentication procedures
      (i) Unique user ID requirement
      (ii) Password standards
      (iii) Others
   (c) Individual user identity-proofing requirements
   (d) Other authentication procedures, if any

16. Access Controls

(a) Repeated failed access attempts
(b) Automatic log-off
(c) Remote access rules

17. Virus Protection

(a) By HIE
(b) By covered entities and business associates

18. Transmission Security

(a) Encryption
(b) Other integrity controls, if any

19. Privacy and Security Training

(a) Content of training
(b) Frequency of training
(c) Responsibility for training covered entity, business associate and HIE users
(d) Documentation of training

20. Auditing

(a) Content of audit logs
(b) Retention and integrity of audit logs
(c) Scope of audits
(d) Frequency of audits
(e) Responsibility for auditing
(f) Reporting of audit findings, including whether to report findings to patients and/or the public
(g) Corrective action

Violations and Enforcement

21. Breach Notification

(a) Definition of breach
(b) Reporting and notification obligations
(c) Cost of notification
(d) Remediation

22. Sanctions

(a) Conduct triggering sanctions
(b) Types of sanctions for covered entities, business associates and individual users
(c) Process for carrying out sanctions (e.g. dispute resolution procedures, termination procedures etc.)

* * * *